New York City District Council of Carpenters Pension Fund v. SolarWinds Corporation

COURT: United States District Court for the Western District of Texas
CASE NUMBER: 1:21-cv-00138
CLASS PERIOD: 10/18/2018 - 12/17/2020
CASE LEADERS: John Rizio-Hamilton, Hannah Ross, Jonathan D. Uslaner
CASE TEAM: Will Horowitz, Thomas Sperber

On February 9, 2021, after an extensive investigation and a careful evaluation of the merits of this case, Bernstein Litowitz Berger & Grossmann filed a class action lawsuit on behalf of its client, the New York City District Council of Carpenters Pension Fund, and all others similarly situated, for violations of the federal securities laws in the U.S. District Court for the Western District of Texas against SolarWinds Corporation ("SolarWinds" or the "Company") certain of the Company's current and former senior executives, and two private equity firms that controlled SolarWinds during the Class Period (collectively, "Defendants").

On March 11, 2021, the New York City District Council of Carpenters Pension Fund was appointed Lead Plaintiff for the Class, and BLB&G was appointed Lead Counsel. Lead Plaintiff filed a consolidated complaint on June 1, 2021 on behalf of investors in SolarWinds common stock between October 18, 2018 and December 17, 2020, inclusive (the "Class Period"). On March 30, 2022, the Court largely denied the defendants' motion to dismiss. The case will now proceed to discovery.

SolarWinds' Alleged Fraud

Based in Austin, Texas, SolarWinds provides network management software used to monitor and manage networks, systems, and applications. The Company's flagship product is its Orion platform. SolarWinds sells network monitoring software to a significant portion of the United States federal government and the majority of Fortune 500 companies in the United States. Its customers include the U.S. Pentagon, State Department, the Office of the President of the United States, the FBI, the Secret Service, and the National Nuclear Security Administration—customers whose data is among the most sensitive in the world.

Throughout the Class Period, SolarWinds and its top executives sought to leverage customer concerns by touting their commitment to cybersecurity and expertise in the cybersecurity space. The Company showcased its "Security Resource Center" on its website, which compiled information about cybersecurity trends and recommended best practices to keep its customers safe from cyberattacks. The Company assured customers and investors that it was not only committed to cybersecurity but also followed specific practices to ensure the security of its products—and, by extension, customers' data. Featured prominently in its Security Resource Center, and accessible from any page on the website, was the Company's Security Statement, which contained a series of representations regarding the Company's cybersecurity. In addition, the Company's chief security spokesman—Defendant Tim Brown—spoke frequently about the Company's supposed cybersecurity.

Unknown to investors at the time, the Company knew prior to the Class Period that its internal cybersecurity practices were woefully deficient and not as represented. Ian Thornton-Trump, SolarWinds' former Global Cybersecurity Strategist explained that the Company failed to follow a host of basic cybersecurity practices. In April

2017, Mr. Thornton-Trump convened several of the Company's top executives and gave a presentation on the Company's deficient cybersecurity practices. During his presentation, Mr. Thornton-Trump stressed that changes were necessary, warning that "[t]he survival of our customers depends on a commitment to build secure solutions" and "[t]he survival of the company depends on an internal commitment to security." The Company refused to implement the changes in Mr. Thornton-Trump's presentation because the Company's then-CEO, Defendant Kevin Thompson, did not want to spend the money to do so. Mr. Thornton-Trump resigned in protest. In addition to Mr. Thornton-Trump, a host of former SolarWinds employees have explained that the Company lacked the cybersecurity protections it claimed to have in its "Security Statement."

The Company's deficient cybersecurity practices exposed the Company to cyberattack throughout the Class Period. On November 11, 2019, a cybersecurity researcher notified the Company in writing that the password to its Update Server—the server from which customers downloaded software updates for the Company's products—had been publicly available on the internet for approximately one-and-a-half years. On June 17, 2018, a SolarWinds employee—later identified by the Company as an intern—had posted the password along with credentials and a link to the Update Server on a public website. In addition to being publicly available, the password to access the Update Server was "solarwinds123."

Investors first began to learn about the Company's deficient cybersecurity practices on December 13, 2020, when it was leaked to the press that cybercriminals had entered SolarWinds' systems and used its Update Server to execute the largest cyberattack in U.S. history. Cybercriminals—who had unfettered access to the Company's server for nearly two years prior to this disclosure—injected malicious code into a SolarWinds software update, which was then disseminated to tens-of-thousands of the Company's customers via the Update Server. After the revelation of the cyberattack, a full picture of the Company's deficient cybersecurity practices became public.

Investors suffered immensely as a result of the Company's misrepresentations and omissions. As the truth was revealed over the course of several disclosures, the price of SolarWinds' stock cratered. All told, over the course of just a few days, the Company's share price plummeted 34%. Meanwhile, Defendants profited handsomely. From the beginning of the Class Period, Defendants reaped $730 million in proceeds from their sales of SolarWinds stock, including through the private equity firms' sale of over $450 million in their own stock, less than seven days before the initial disclosures that caused investors' substantial losses.

Case Documents

- June 1, 2021 - Consolidated Class Action Complaint
- February 9, 2020 - Initial Complaint
- February 9, 2020 - PSLRA Notice